⑲ Japanese Patent Office (JP)
⑪ Japanese Utility Model Application Publication No. S63-314586
⑫ Publication of Unexamined Patent Application (A)
⑤① Int. Cl. [4] Identification No. Code No. in JPO
G 09 C 1/00 G 7368-5B
④③ Published on December 22, 1988

Request for Examination: Not yet requested.
Number of Claims: 2 (6 pages)

---

⑥④ Title of the Invention: Encryption Method
②① Japanese Utility Model Application No. S62-151840
②② Application Filed on June 17, 1987
⑦② Creator of Device: Eiji Okamoto
NEC Corporation
5-33-1,Shiba, Minato-ku,
Tokyo
⑦① Applicant: NEC Corporation
5-33-1, Shiba, Minato-ku, Tokyo
⑦④ Attorney: Patent Attorney Shin Uchihara

Specification

Title of the Invention

Encryption Method

What is claimed is

1. An encryption method in a network having a center and a terminal for encrypting or decrypting data transmitted from the terminal to the center, the method comprising the steps of:

encrypting the data in the terminal using a key generated therein by using a digital pattern previously determined for the terminal and a random pattern generated randomly;

generating key generating information in the terminal by using a pattern kept in secret and the random pattern;

transmitting the encrypted data and the key generating information to the center; and

decrypting the encrypted data in the center using a key generated therein by using the key generating information, identified information corresponding to the terminal or a user using the terminal, and a pattern previously determined.

2. An encryption method in a network having a center and a terminal for encrypting or decrypting data transmitted from the center to the terminal, the method comprising the steps of:

requesting from the terminal to the center to transmit the data by sending a key generating information from the terminal to the center, the key generating information generated therein by using a pattern kept in secret and a random pattern generated randomly;

encrypting the data in the center using a key generated therein by using the key generating information, identified information corresponding to the terminal or a user using the terminal, and a pattern previously determined;

transmitting the encrypted data from the center to the terminal; and

decrypting the encrypted data in the terminal using a key generated therein by using the random pattern, a pattern previously determined.

Industrial Field of the Invention

The present invention relates to the encryption method for a network having a center and a terminal, more specifically to a method of encrypting data transmitted from the terminal to the center or inversely from the center to

the terminal.

Related Art and Problems thereof

In encrypted communications, transmitting a key is necessary. A known method for transmitting a key is the public key distribution method.(IEEE Transactions on Information Theory Volume22 Number6 page644 to654). This method, however, has the problem that a public information list becomes larger in proportion to the number of members. As a method to solve the problem, Japanese Patent Application NO. S61-197611 disclosed a method. This method, however, was adapted to multidirectional communications and can not be used an Electronic Bulletin Board System in which a bulletin board is provided in the center.

Means to Solve the Problems

The present invention provides a method including the steps of, encrypting the data in the terminal using a key generated therein by using a digital pattern previously determined for the terminal and a random pattern generated randomly; generating key generating information in the terminal by using a pattern kept in secret and the random pattern; transmitting the encrypted data and the key generating information to the center; and decrypting the encrypted data in the center using a key generated therein by using the key generating information, identified information corresponding to the terminal or a user using the terminal, and a pattern previously determined, or a method including the steps of, requesting from the terminal to the center to transmit the data by sending a key generating information from the terminal to the center, the key generating information generated therein by using a pattern kept in secret and a random pattern generated randomly;

encrypting the data in the center using a key generated therein by using the key generating information, identified information corresponding to the terminal or a user using the terminal, and a pattern previously determined; transmitting the encrypted data from the center to the terminal; and decrypting the encrypted data in the terminal using a key generated therein by using the random pattern, a pattern previously determined.

Process

FIG. 1 shows a process and principle according to the present invention. FIG. 1A shows a case when user A transmits data to the center. FIG. 1B shows a case when the center transmits data to user B to respond to a request from the user B. The User A and the user B may be identical. Each user i possesses a secret integer S_i, and also possesses integers α, n, and y which are common among all the users. The center possesses a secret integer r, and also possesses integers, e and n. These integers are previously determined and distributed by a reliable person or organization. A method how to decide will be explained later. For each user i assigned is IDi in which information such as the name and the address are coded. The IDi shall be known to everyone. The expressions E_K(DaTa) and D_K(ED) in the FIGs represent to encrypt the DaTa using a key K and to decrypt the ED using a key K, respectively. Also, the expression a(mode b) represents the remainder when a is divided by b. FIG. 1A and 1B shows the process and principle of claim 1 and claim 2 according to the present invention, respectively.

In FIG. 1A, the user A generates a random number rA, and calculates $IKA=y^{rA}$(mode n) and $XA=SA*\alpha^{rA}$(mode n). The data is encrypted by $ED=E_{IKA}$(DaTa) using the IKA as a key. All the data of the IDA, XA, and ED are transmitted to the center.

The center calculates $IK=(XA^{e}*IDA)^{r}(\text{mod } n)$ and decrypts the ED using IK as a key to obtain data. Namely, $DaTa=D_{IK}(ED)$.

In this case, integers, Si, n, α, e, r, and y are given as follows. N is the product of two prime numbers p and q in which the P and q should be large enough so that the integer n can not be factorized easily. For example, it should be enough if both integers, p and g, are about 2^{256}. The integer e should be a prime number less than the integer n, and the integer α should be a integer less than the integer n. In addition, d is obtained so that the equation $e*d(\text{mod}(p-1)(q-1)=1$ is true, and Si is obtained by the equation $Si=IDi^{-d}(\text{mod } n)$. Also r should be an integer randomly obtained and but should be less than the integer n, and y is obtained by the equation $y=\alpha^{e*r}(\text{mod } n)$. In this case, the equation $IDi=Si^{-e}(\text{mod } n)$ is true. This is described in the magazine, Communication of the ACM, Volume21 Number2 Page120 to 126. Above equations are true since so-called the RSA Public Key Encryption System is employed. Now, the equation $IKA=y^{rA}(\text{mod } n)=\alpha^{e*r*rA}(\text{mod } n)$ is true. On the other hand, the equation $IK=(XA^{e}*IDA)^{r}(\text{mod } n)=(SA^{e}*\alpha^{e*rA}*IDA)^{r}(\text{mod } n)=\alpha^{r*e*rA}(\text{mod } n)$ is true and equal to IKA. Therefore, the original data can be restored by decrypting the ED using IK as a key.

Since the integer Si should be known by the user i only (assuming that the person or organization who generated the Si never leaks the secret information), the XA can be generated by the user A only. Also, since the r is known by the center only, the calculation of the $IK=(XA^{e}*IDA)^{r}(\text{mod } n)$ can be done by the center only. Therefore, IKA=IK can be generated by the user A and the center only. Above description explains the process and principle of the claim 1 according to the present invention.

There are some other methods to generate the IK that

is shown in FIG. 1. For example, as shown below, the user A transmits the data of $ZA=\alpha^{e*rA} \pmod n$ and $WA=SA\,\alpha^{c*rA} \pmod n$. The center then generates the IK from the equation $IK=ZA^{r} \pmod n$ only when the $(ZA^{c}*WA^{e})^{-1} \pmod n = IDA$ is true. When the $(ZA^{c}*WA^{e})^{-1} \pmod n = IDA$ is not true, the key transmission process is then halted because of the possibility of an error or data falsification. In above equations, c represents a constant prime number

FIG. 1B shows a case where the user requests the center to transmit data to the user. In FIG. 1B, the direction of the data transmission is reversed to that in FIG. 1A. However, the method of generating the keys IKB and IK for encrypting data is exactly the same as that shown in FIG 1A. Therefore, when the Si, n, α , e, r, and y are determined in the same manner as in the process shown in FIG. 1A, data can be transmitted as a secret for a third party.

Embodiments

FIG. 2 is a schematic diagram showing a first embodiment according to the present invention. This embodiment shows an example of an Electronic Bulletin Board System (hereinafter BBS) in a personal computer network. There may be some other embodiment such as an e-mail system and a data base system as an embodiment of the present invention, but to simplify the explanations, only BBS is referred in the explanation below.

Each user i has its IC card in which the data of IDi, Si, α, and n are written therein. To access to the BBS, the user A inserts an IC card 213 into a card reader 212 of a terminal 211. Each terminal 211 carry out the process according to the flow chart shown in FIG. 3A. Namely, the terminal 211 reads the data of IDi, Si, α, and n, generates a random number rA, and calculates the XA. In this case,

however, the user A is accessing to the terminal 211, so the symbol i should be replaced by the A (same as blow). To write in the BBS, IKA is calculated, and data to be written in the BBS is encrypted using IKA as a key. The encrypted datam IDA, and XA is transmitted to the BBS. Inversely, to read the information bulletined on the BBS, a transmission request is transmitted to the BBS. The IDA and XA are also transmitted to the BBS when the request is made. Random number rA used later is stored in an appropriate area. On the other hand, as shown in FIG. 3B, when the BBS receives the data to be written on the BBS, the BBS calculates the IK and decrypt the data using the IK and bulletins the decrypted data on the BBS. When receiving a request to read data on the BBS, the BBS calculates the IK and encrypt the data using the IK as a key and transmit the encrypted data. Again refer to FIG. 3A again. When the terminal receives the data from the BBS, the terminal calculates the IKA using the rA previously stored therein, and decrypts the data. Also, it may be preferable to calculate the IKA before the data is received from the BBS.

FIG. 4 is a configuration diagram showing a second embodiment according to the present invention. This embodiment is an example of an e-mail system in a personal computer network. There are some other examples such as an electronic bulletin board system and a data base file system as an embodiment of the present invention.

Each user i has its IC card in which the data of IDi, Si, α, and n are written therein. A case when a user A transmits a mail to a user B is explained. The user A inserts an IC card 413 into a card reader 412 of a terminal 411. Ecah terminal carries out the process according to the flow chart shown in FIG. 5A. Namely, the terminal 411 reads the data of IDi, Si, α, and n, generates a random number rA and WK, and calculates the XA and IKA. In this case, however, the

user A is accessing to the terminal 411, so the i should be replaced by the A (same as blow). The work key WK is encrypted using the IKA as a key to generate the EKA, and the mail is encrypted using the WK. The encrypted mail as well as IDA, IDB, XA, and EKA are transmitted to a mail center 430. The IDj in the FIG. represents the identification data of the mail receiving user. The mail center 430 carries out the process according to the flow chart in FIG. 5B. Namely, when receiving the encrypted mail as well as IDA, IDB, XA, and EKA, the mail center calculates the IKA fromh the XA and the IDA, and obtain the WK from the equation $WK=D_{IKA}(EKA)$, and stores the WK and the encrypted mail into a mail box 432 for the user B. When the user B requests to read a mail to the user B, the user B inserts an IC card 423 into an IC card reader 422 of an arbitrary terminal (terminal 421 in this case). As shown in FIG. 5A, the terminal 421 reads the data of SB, IDB, α, and n, generates a random number rA and calculates the XB, and transmits the IDB and VB to the mail center 430 to request to read a mail. As shown in FIG. 5B, the mail center 430 calculates the IKB, and generates the EKB by encrypting, using the IKB, the WK that was read from the mail box of the user B. The mail center 430 transmits the EKB and the encrypted mail to the terminal 422. Also, it may be preferable to calculate IKB before the encryption is received from the mail center.

In this embodiment, the work key WK and the encrypted mail are stored into the mailbox of the mail center. To ensure the security, it is possible to store the work key in a different area or to decide a unique key for the mail center, MK, and the WK is encrypted using the MK and saved in the same box.

In above explanations of embodiments, the Si, α, n, y, e, r are assumed as the constant values. As a measure to

deal with the accidents that both the IC cards and secret information are stolen, an expiration date can be set to some of the above parameters. For example, the Si can be give as $Si=(IDi,year)^d$. Herein, (IDi,year) represents a pattern consisting of patterns of IDi and year. Also an expiration date can be set to the other constant numbers like n. Or it is also possible to add an embodiment in which the users are divided into groups: for each group, each key is distributed among the users in each group, and in the same group, a conventional key distribution or a method according to the present invention is used. Those are included in the scope of the present invention.

Advantages of the present Invention

As explained above in detail, according to the present invention, there is provided a method of encryption communications in which each user and a center advantageously keep only limited amount of data stored therein.

Brief Description of the Drawings

FIG. 1A and 1B are drawings showing the process and principle according to the present invention;

FIG. 2 and 4 are the schematic diagrams showing a first and a second embodiments according to the present invention, respectively; and

FIG. 3A, 3B and 5A , 5B are flow charts explaining the processes to be carried out by a terminal and a center, respectively.

Among the FIGs, reference number 201 denotes an Electronic Bulletin Board System (BBS); 211, 411, and 421 denote a terminal; 212,412, and 422 denote a card reader; 213,413, and 423 denote an IC card; 430 denotes a mail center;

and 432 denotes a mail box.

Drawings

FIG. 1A

①

Random Number rA Generation

②

$IKA=y^{rA}(\text{mod } n)$ Calculation

③

$ED=E_{IKI}(DaTa)$

④

$XA=SA*\alpha^{rA}(\text{mod } n)$ Calculation

⑤

(IDA,XA,ED) Transmission

Processes in User A side

⑥

(IDA,XA,ED) Reception

⑦

$IK=(XA^{e}*IDA)^{r}(\text{mod } n)$ Calculation

⑧

$DaTa=D_{IK}(ED)$

Processes in Center side

FIG. 1B

①

Random Number rB Generation

②

$XB=SB*\alpha^{rB}(\text{mod } n)$ Calculation

③

(IDB,XB) Transmission

④

(IDB,XB) Reception

⑤

$Ik=(XB^{e}*IDB)^{r}(\mathrm{mod}\ n)$ Calculation

⑥

$ED=E_{IK}(DaTa)$

⑦

ED Transmission

Processes in Center side

⑧

ED Reception

⑨

$IKB=y^{rB}(\mathrm{mod}\ n)$

⑩

$DaTa=D_{IKB}(ED)$

Processes in User B side

FIG. 2

Bulletin Board

FIG. 3A

BBS Write Request

Read Card Information

Generate Random Number ri

Calculate Xi and Iki

Encrypt Data

Transmit IDi, Xi, Encrypted Data

EXIT

BBS Read Request

Read Card Information

Generate Random Number ri

Calculate Xi

Transmit IDi, Xi, Transmission Request

Store ri

EXIT

Receive Encrypted Data

Calculate Iki

Decrypt Encrypted Data

EXIT

FIG. 3B

Receive IDi, Xi, Encrypted Data

Calculate Iki

Decrypt Encrypted Data

Write Data on BBS

EXIT

Receive BBS Read Request

Calculate Iki

Encrypt Data

Receive Encrypted Data

EXIT

FIG. 4

IC Card

FIG. 5A

Mail Transmission Request

Read Card Information

Generate Random number ri, wk

Calculate Xi, Iki

$Eki=D_{Iki}(WK)$

Destination Mail Receipt

Encrypt Mail

Transmit IDi, IDj, Xi, Eki, Encrypted Mail

EXIT

Mail Receipt Request

Read Card Information

Generate Random Number ri

Calculate Xi

Transmit IDi, Xi

Store ri

EXIT

Receive Encrypted Mail

Calculate Iki

$wk=D_{Iki}(Eki)$

Decrypt Mail

EXIT

FIG. 5B

Receive IDi, IDj, Xi, Eki, Encrypted Mail

Calculate Iki

$wk=D_{Iki}(Eki)$

Store WK and Encrypted Mail into Mail Box for j

EXIT

Receive Mail Reception Request

Calculate Iki

Read wk, Encrypted Mail from Mail Box

$Eki=E_{Iki}(wk)$

Transmit Eki, Encrypted Mail

EXIT

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－314586

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開 昭和63年(1988)12月22日
G 09 C 1/00		7368－5B	

審査請求 未請求 発明の数 2 （全6頁）

㊹発明の名称　暗号化方式

㉑特　願　昭62－151840
㉒出　願　昭62(1987)6月17日

㉒発明者　岡本　栄司　東京都港区芝5丁目33番1号　日本電気株式会社内
㉑出願人　日本電気株式会社　東京都港区芝5丁目33番1号
㉔代理人　弁理士 内原　晋

明　細　書

発明の名称　暗号化方式

特許請求の範囲

1．センターと端末からなるネットワークで、端末からセンターへ送るデータを暗号化あるいは復号化するために、端末においてはあらかじめ定められたディジタルパターンとランダムに発生したランダムパターンとに依存して生成したキーで前記データを暗号化し、秘密に保持しているパターンと前記ランダムパターンとに依存して作成したキー作成用情報と共に該暗号化データをセンターに送り、前記センターにおいては前記キー作成用情報と前記端末あるいは該端末を使用しているユーザに対応した識別情報とあらかじめ定められたパターンとに依存して作成したキーで前記暗号化データを復号化することを特徴とする暗号化方式。

2．センターと端末から成るネットワークで、センターから端末へ送るデータを暗号化あるいは逆に復号化するために、端末はセンターにデータを要求する際に、秘密に保持しているパターンとランダムに発生したランダムパターンとに依存して生成したキー作成用情報を前記センターに送り、前記センターは前記キー作成用情報と前記端末あるいは該端末を使用しているユーザに対応した識別情報とあらかじめ定められたパターンとに依存して作成したキーで前記データを暗号化して前記端末に送り、前記端末は前記ランダムパターンとあらかじめ定められたパターンとに依存して作成したキーで前記の暗号化データを復号化することを特徴とする暗号化方式。

発明の詳細な説明

（産業上の利用分野）

本発明は、センターと端末から成るネットワークにおいて、端末からセンターへ送るデータの暗号化、あるいは逆にセンターから端末へ送るデータの暗号化に関する。

（従来技術とその問題点）

暗号通信ではキー配送が必要となるが、従来から知られているキー配送方式としては公開鍵配送方式が有名である（アイ　イー　イー　イー・トランザクションズ・オン・インフォーメーション・セオリー（IEEE Transactions on Information Theory）22巻６号　644頁～　654頁）。しかしこの方式は公開情報リストの大きさが加入者数に比例する欠点がある。この欠点を解決する方法として、特願昭61-197611 号に記載のものがある。しかしこの技術は多方向通信用であり、センターに掲示板があるような電子掲示板システムには使えない。

（問題点を解決するための手段）

本発明は、端末においてはあらかじめ定められたディジタルパターンとランダムに発生したランダムパターンとに依存して生成したキーで前記データを暗号化し、秘密に保持しているパターンと前記ランダムパターンとに依存して作成されたキー作成用情報と共に暗号化データをセンターに送り、前記センターにおいては前記キー作成用情報と前記端末あるいは該端末を使用しているユーザに対応した識別情報とあらかじめ定められたパターンとに依存して作成したキーで前記暗号化データを復号化することを特徴とする暗号化方式、またはセンターと端末から成るネットワークで、センターから端末へ送るデータを暗号化あるいは逆に復号化するために、端末はセンターにデータを要求する際に、秘密に保持しているパターンとランダムに発生したランダムパターンとに依存して生成したキー作成用情報を前記センターに送り、前記センターは前記キー作成用情報と前記端末あるいは該端末を使用しているユーザに対応した識別情報とあらかじめ定められたパターンとに依存して作成したキーで前記データを暗号化して前記端末に送り、前記端末は前記ランダムパターンとあらかじめ定められたパターンとに依存して作成したキーで前記の暗号化データを復号化することを特徴とする暗号化方式である。

（作用）

第１図は本発明の作用・原理を示す図である。

第１図(a)はユーザＡがセンターにデータを送る場合、第１図(b)がユーザＢの要求によりセンターからユーザＢへデータを送る場合である。ＡとＢは同一のこともありうる。各ユーザｉは秘密整数Siを持ち、さらに全ユーザ共通の整数α、ｎ、ｙを持つ。センターは秘密整数ｒと他に整数ｅ、ｎを持つ。これらの整数はあらかじめ信頼できる人又は機関が定めて配っておく。定め方は後述する。また各ユーザｉには氏名や住所などをコード化したIDi が対応していて、このIDi は誰でも知っているものとする。図におけるE_K(DaTa)、D_K(ED)は各々、DaTaをキーＫで暗号化すること及びEDをキーＫで復号化することを示す。また、a(mod b)はａをｂで割った余りを意味する。第１図(a)が第１の発明、第１図(b)が第２の発明の作用・原理を示している。

第１図(a)において、ユーザＡは乱数rAを生成し、$IKA=y^{rA} \pmod n$ と$XA=SA\cdot\alpha^{rA} \pmod n$ を計算する。IKA をキーとしてデータを $ED=E_{IKA}$(DaTa)で暗号化し、(IDA,XA,ED) をセンターに送る。センターは$IK=(XA^{e}\cdot IDA)^{r} \pmod n$を計算し、IKをキーとしてEDを復号化してデータを得る。即ち、$DaTa=D_{IK}(ED)$。

ここで、Si、ｎ、α、ｅ、ｒ、ｙを次のように定めておく。ｎは２つの素数ｐ，ｑの積で、ｎの因数分解が困難な程度にｐ，ｑの大きさを定める。例えばｐ，ｑとも2^{256}程度なら十分である。ｅをｎ未満の素数とし、αはｎ未満の整数とする。さらにｄを$e\cdot d \pmod{(p-1)(q-1)}=1$となるように定め、$Si=IDi^{-d} \pmod n$ とする。また、ｒはランダムに定めたｎ未満の整数とし、$y=\alpha^{e\cdot r} \pmod n$とおく。このとき $IDi=Si^{-e} \pmod n$となる。これは雑誌コミュニケーション・オブ・ザ・エーシーエム(Communication of the ACM)21巻２号 120頁～126 頁に記載されている、いわゆる RSA公開鍵暗号系を用いているので、成立する。さて、$IKA=y^{rA} \pmod n=\alpha^{e\cdot r\cdot rA} \pmod n$ であり、一方 $IK=(XA^{e}\cdot IDA)^{r} \pmod n=(SA^{e}\cdot\alpha^{e\cdot rA}\cdot IDA)^{r} \pmod n=\alpha^{r\cdot e\cdot rA} \pmod n$ で IKAと等しくなる。従ってEDをIKをキーとして復号すれば元のデータに戻る。

Siはユーザiのみが知っている（但し、Siを作成した信頼できる人又は機関は不正を働かないとする）のでXAはユーザAしか作れない。また、rはセンターのみが知っているので、IK=(XA^ID)^r (mod n) の処理をできるのはセンターだけである。従ってIKA=IKはユーザAとセンターのみが作れる。以上により、第1の発明の動作・原理が示された。

なお、IKの生成法には第1図に示す他にもある。例えば次例に示す通りである。ユーザAはZA= α^rA(mod n) とWA=SA・α^rA(mod n) を送り、センターでは(ZA^・WA^)^-1(mod n)=IDAならばIK=ZA^r(mod n) からIKを作るというようにする。(ZA^・WA^)^-1(mod n)=IDAならば誤まりか改ざんがあったとしてキー配送処理を中断する。ここでcはある一定の素数である。

第1図(b)はユーザからセンターにデータを要求する場合である。図において、データの送信が第1図(a)と逆になっている。しかし、データ暗号化用キーIKBとIKの作成方法は第1図(a)と全く同じである。従って、Si、n、α、e、r、yを第1図(a)と同様に定めれば、第3者に秘密にデータを転送できる。

（実施例）

第2図は本発明の第1の実施例を示す構成図である。本実施例ではパーソナルコンピュータ・ネットワークにおける電子掲示板システム（以下BBSと記す）に本発明を実施した例である。他にも電子メールシステムやデータベースシステムにも実施できるが、説明を簡単にするためBBSのみで説明する。

各ユーザiはIDi、Si、α、nを書込んであるICカードを保持する。ユーザAがBBSにアクセスする場合には、ある端末211のカード・リーダ212にICカード213を差し込む。各端末211は第3図(a)に示すフローチャートに従って処理を行なう。即ち、ICカードからSA、IDA、α、nを読込み、乱数rAを生成してXAを計算する。なお、今はユーザAが端末211にアクセスしているのでiはAである。以下同じ。もし、BBSへの書込の場合にはIKAを計算し、IKAをキーとしてBBSに書込むべきデータを暗号化してIDA、XAと共にBBSに送る。逆にBBSに掲示されている情報を読む場合には、BBSに送信要求を出すが、その際にIDAとXAも送り、あとで用いる乱数rAを適当な場所に格納する。一方、BBSでは第3図(b)に示す通り、まず、書込データを送られた場合には、IKを計算し、それで暗号文を復号化して掲示板に書く。もし、掲示板の閲覧要求ならば、まずIKを計算し、それで掲示板のメッセージを暗号化して送る。再び第3図(a)に戻り、BBSから暗号文が送られれば、先に格納していたrAを用いてIKAを計算し、送られた暗号文を復号化する。なお、IKAはBBSからの暗号文が到着する前に計算しておいてもよい。

第4図は本発明の第2の実施例を示す構成図である。本実施例ではパーソナルコンピュータネットワークにおける電子メールシステムに本発明を実施した例である。他にも電子掲示板システムやデータベースファイルシステムにも適用できる。

各ユーザiはIDi、Si、α、nを書込んであるICカードを保持する。ユーザAがユーザBにメールを送るとして説明する。ユーザAはある端末411のカードリーダ412にICカード413を差込む。各端末は第5図(a)に示すフローチャートに従って処理を行なう。即ち、ICカードからSA、IDA、α、nを読込、乱数rAとWKを生成してXA、IKAを計算する。なお、今ユーザAが端末411にアクセスしているので図中のiはAとなる。以下同じ。IKAをキーとしてワークキーWKを暗号化したものをEKAとし、WKでメールを暗号化する。そして該暗号化メールをIDA、IDB、XA、EKAと共にメールセンター430に送る。図中IDJはメール受信ユーザの識別情報である。メールセンター430は第5図(b)に示すフローチャートに従って処理を行なう。即ち、ユーザAからIDA、IDB、XA、EKA及び暗号メールを受信すると、XA、IDAからIKAを計算し、WK=D_IKA(EKA)からWKを求める。このWKと暗号メールをユーザBへのメールボックス432に格納する。ユーザBが自分宛のメール文を要求する場合に

は、任意の端末（ここでは421とする）のICカードリーダ422にICカード423を差込む。端末421は第5図(a)に示すようにICカードからSB、IDB、α、nを読込み、乱数rBを生成してXBを計算する。そしてメールセンター430にIDB、XBを送ってメール要求を行なう。メールセンター430は第5図(b)に示すように、IKBを計算し、B宛のメールボックスから読出したWKをIKBで暗号化したEKBと暗号メールを端末421に送る。端末421は第5図(b)に示すように、EKBと暗号メールを受取るとIKBを計算しWK=D_{IKB}(EKB)からワークキーWKを求める。このWKを用いて暗号メール文を復号化して元のメールを得る。なお、IKBはメールセンターから暗号メールが到着する前に計算しておいてもよい。

本実施例においてメールセンターのメールボックスにワークキーWKと暗号メールを格納するとして説明してきたが、安全のため、ワークキーはメールボックスとは別の場所に格納するか又は、メールセンター固有のキーMKを定め、MKでWKを暗号化してメールボックスに格納しておくことができる。

以上の実施例の説明において、SI、α、n、y、e、rは一定として説明したが、ICカード盗まれしかもICカードの暗証情報も盗まれた時の対策として、上記パラメータの幾つかに有効期限を設けることができる。例えばSI=(IDI,年号)^e (mod n)とすればよい。ここで、(IDI,年号)はIDIと年号のパターンを並べたパターンである。他のnなども有効期限を設けることが可能である。また、ユーザをグループ分けし、各グループ毎に本発明方式で示したキー配送を行ない、グループ間では従来のキー配送方式や本発明方式を用いるという実施例もある。これらは本発明の範囲に含まれる。

（発明の効果）

以上詳細に説明したように、本発明を用いれば、各ユーザ及びセンターはわずかな情報をもつだけで暗号通信ができるという効果を生じる。

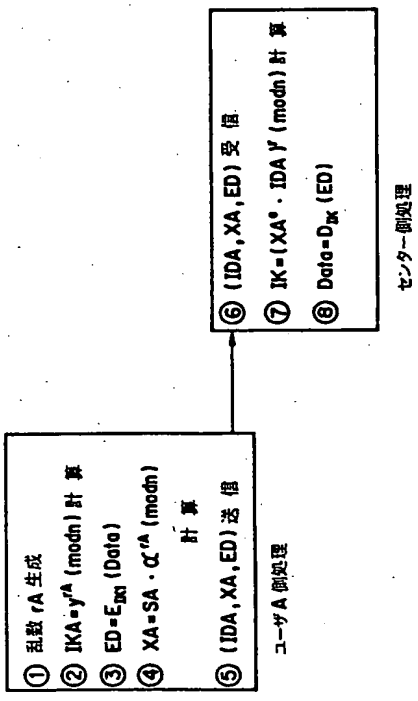
図面の簡単な説明

第1図(a),(b)は本発明の作用・原理を示すための図、第2図、第4図は各々本発明の第1、第2の実施例を示す構成図、第3図(a),(b)を第5図(a),(b)は各々第2図と第4図の端末とセンターがなすべき処理を示すフローチャート、である。

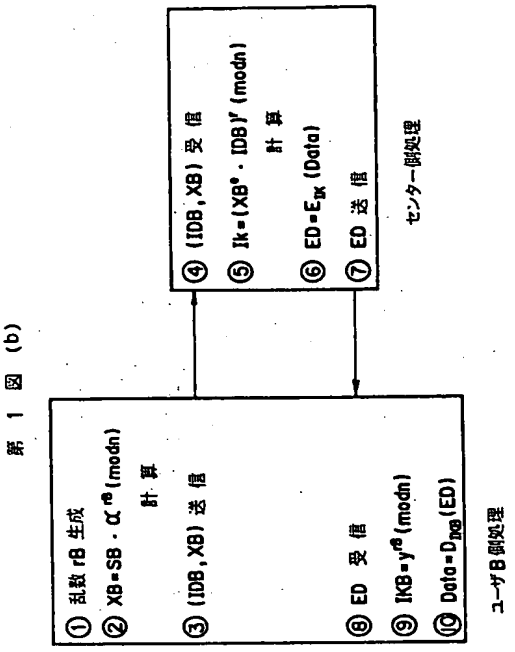
図において、201は電子掲示板、211,411,421は端末、212,412,422はカードリーダ、213,413,423はICカード、430はメールセンター、431,432はメールボックスを各々示す。

代理人　弁理士　内原　晋

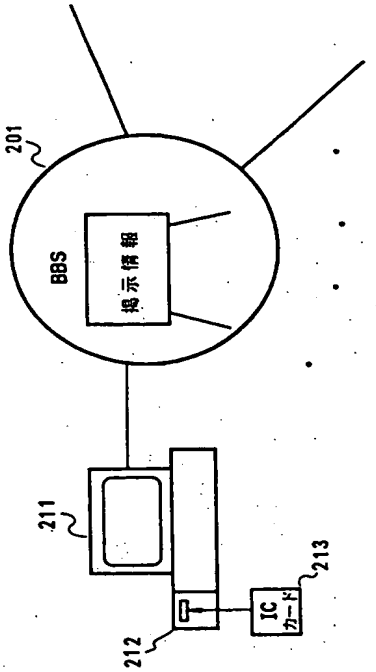
第1図(a)



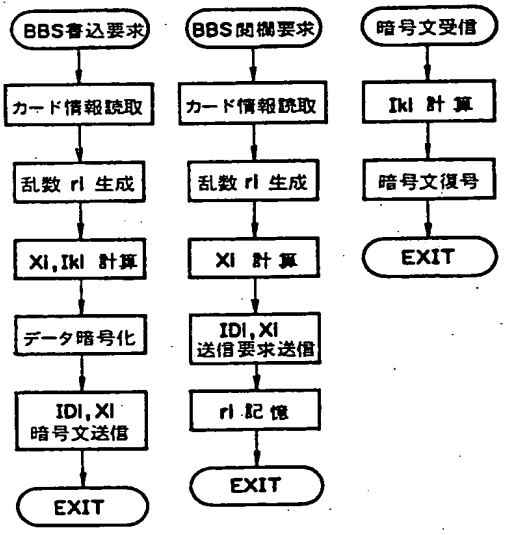
第 1 図 (b)



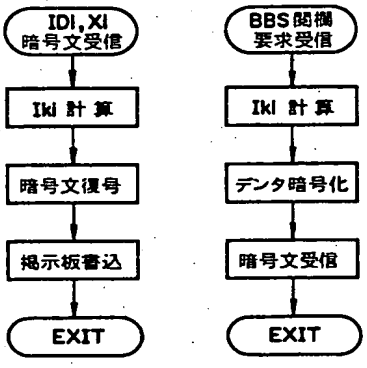
第 2 図

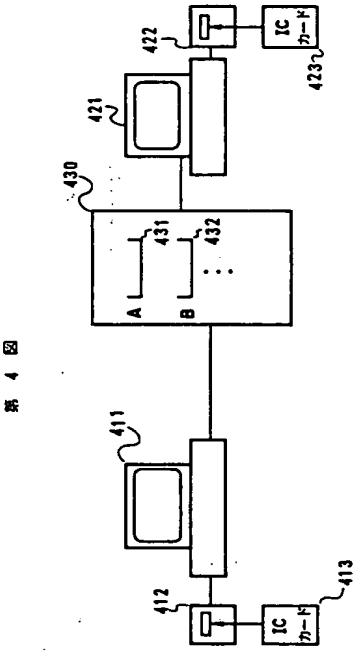


第 3 図 (a)



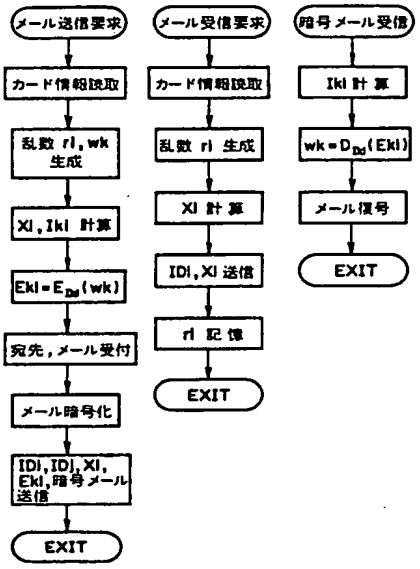
第 3 図 (b)





第 4 図

第 5 図 (a)



第 5 図 (b)